1 CLAIMS

2 Having thus described my invention, what I claim as new and desire to secure by Letters
3 Patent is as follows:

4 1. A method for encrypting a plain-text message, the method comprising:

5 generating a first random number;

6 transforming said first random number into a first pseudo random number;

7 further expanding a randomness of said first random number and/or said first pseudo
8 random number into a set of pair-wise differentially-uniform pseudo random numbers;

9 dividing said plain-text message into a plurality of plain-text blocks;

10 encrypting said plain-text blocks to form a plurality of cipher-text blocks;

11 combining said plurality of plain-text blocks into at least one check sum; and

12 employing said set of pair-wise differentially-uniform pseudo random numbers, together
13 with said first random number and/or said first pseudo random number, to embed a
14 message integrity check in said cipher-text blocks.

15 2. A method as recited in claim 1, wherein the step of encrypting said plain-text blocks
16 includes employing the said first random number, and/or said first pseudo random
17 number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

1   3. A method as recited in claim 1, wherein the step of employing includes pairing said

2   first random number, and/or said first pseudo random number, and/or said set of pair-wise

3   differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks;

4   and

5   combining each pair to form a plurality of output blocks.

6   4. A method as recited in claim 3, wherein the step of combining each pair includes

7   performing an exclusive-or operation upon components of said each pair.

8   5. A method as recited in claim 1, wherein the step of encrypting includes encrypting

9   said first random number.

10   6. A method as recited in claim 1, wherein the step of encrypting includes encrypting said

11   check sum.

12   7. A method as recited in claim 1, wherein the step of combining includes obtaining said

13   check sum from an exclusive-or of said plurality of plain-text blocks.

14   8. A method as recited in Claim 1, wherein the step of transforming said random number

15   includes a non-cryptographic or linear operation.

16   9. A method as recited in Claim 1, wherein the step of transforming said random number

17   includes a cryptographic operation.

18   10. A method as recited in Claim 1, wherein the said set of pair-wise

19   differentially-uniform numbers are set of pair-wise differentially-uniform numbers in

20   GFp.

21   11. A method as recited in claim 2, wherein the step of employing includes:

1   pairing said first random number, and/or said first pseudo random number, and/or said set

2   of pair-wise differentially-uniform pseudo random numbers, with said plurality of

3   plain-text blocks; and

4   combining each pair to form a plurality of input blocks used in said step of encrypting.

5   12. A method as recited in claim 11, wherein the step of combining each pair includes

6   performing an exclusive-or operation upon components of said each pair.

7   13. A method for decrypting a cipher-text message, the method comprising:

8   dividing said cipher-text message into a plurality of cipher-text blocks;

9   decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

10   transforming at least one of said plain-text blocks into a first pseudo random number;

11   further expanding at least one of said plain-text blocks and/or said first pseudo random

12   number into a set of pair-wise differentially-uniform pseudo random numbers;

13   combining said first pseudo random number, and/or said set of pair-wise

14   differentially-uniform pseudo random numbers, and/or said at least one plain-text block

15   to form at least two check sums and to form a plurality of output blocks; and

16   comparing said at least two check sums in declaring success of a message integrity check.

17   14. A method as recited in claim 13, wherein the step of decrypting said cipher-text

18   blocks includes employing said first pseudo random number, and/or said set of pair-wise

19   differentially-uniform pseudo random numbers.

1   15. A method as recited in claim 13, wherein the step of combining includes:

2   pairing said first pseudo random number, and/or said set of pair-wise

3   differentially-uniform pseudo random numbers, with said plurality of plain-text blocks;

4   and

5   using each pair to form a plurality of output blocks and employing the output blocks to

6   form said at least two check sums.

7   16. A method as recited in claim 15, wherein the step of using each pair includes

8   performing an exclusive-or operation upon components of said each pair.

9   17. A method as recited in claim 15, wherein the step of forming includes:

10   dividing the said output blocks into at least two subsets, and

11   obtaining said at least two checksums from an exclusive-or of said subsets of output

12   blocks.

13   18. A method as recited in Claim 13, wherein the step of transforming said plain-text

14   blocks includes a non-cryptographic or linear operation.

15   19. A method as recited in Claim 13, wherein the step of transforming said plain-text

16   blocks includes a cryptographic operation.

17   20. A method as recited in Claim 13, wherein the said set of pair-wise

18   differentially-uniform numbers are set of pair-wise differentially-uniform numbers in

19   GFp.

1   21. A method as recited in claim 14, wherein the step of employing includes:

2   pairing said first random number, and/or said first pseudo random number, and/or said set
3   of pair-wise differentially-uniform pseudo random numbers, with said plurality of
4   cipher-text blocks; and

5   combining each pair to form a plurality of input blocks used in said step of decrypting.

6   22. A method as recited in claim 3, wherein p is a prime number, and the step of
7   combining each pair includes performing a modulo p addition upon components of said
8   each pair.

9   23. A method as recited in claim 11, wherein p is a prime number, and the step of
10   combining each pair includes performing a modulo p addition upon components of said
11   each pair.

12   24. A method as recited in claim 15, wherein p is a prime number, and the step of using
13   each pair includes performing a modulo p addition upon components of said each pair.

14   25. A method as recited in claim 21, wherein p is a prime number, and the step of
15   combining each pair includes performing a modulo p addition upon components of said
16   each pair.

17   26. An article of manufacture comprising a computer usable medium having computer
18   readable program code means embodied therein for causing encryption of a plain-text
19   message, the computer readable program code means in said article of manufacture
20   comprising computer readable program code means for causing a computer to effect the
21   steps of claim 1.

1   27. An article of manufacture comprising a computer usable medium having computer

2   readable program code means embodied therein for causing decryption of a cipher-text

3   message, the computer readable program code means in said article of manufacture

4   comprising computer readable program code means for causing a computer to effect the

5   steps of claim 13.

6   28. A computer program product comprising a computer usable medium having

7   computer readable program code means embodied therein for causing encryption of a

8   plain-text message, the computer readable program code means in said computer program

9   product comprising computer readable program code means for causing a computer to

10   effect the steps of claim 1.

11   29. A computer program product comprising a computer usable medium having

12   computer readable program code means embodied therein for causing decryption of a

13   plain-text message, the computer readable program code means in said computer program

14   product comprising computer readable program code means for causing a computer to

15   effect the steps of claim 13.

16   30. A program storage device readable by machine, tangibly embodying a program of

17   instructions executable by the machine to perform method steps for encrypting a

18   plain-text message, said method steps comprising the steps of claim 1.

19   31. A program storage device readable by machine, tangibly embodying a program of

20   instructions executable by the machine to perform method steps for decrypting a

21   cipher-text message, said method steps comprising the steps of claim 13.

22   32. A method for encryption/decryption of a plain-text message, the method comprising

23   the steps of:

24   generating a first random number;

1 transforming said first random number into a first pseudo random number;

2 further expanding a randomness of said first random number and/or said first pseudo

3 random number into a set of pair-wise differentially-uniform pseudo random numbers;

4 dividing the plain-text message into a plurality of plain-text blocks;

5 encrypting said plain-text blocks in forming a plurality of cipher-text blocks;

6 combining said plurality of plain-text blocks into at least one check sum; and

7 employing said first random number, said first pseudo random number and said set of

8 pair-wise differentially-uniform pseudo random numbers to embed a message integrity

9 check in said cipher-text blocks to form a cipher-text message; and

10 dividing said cipher-text message into a plurality of cipher-text blocks to form an

11 encryption of said plain-text message;

12 decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

13 transforming at least one of said plain-text blocks into a first pseudo random number;

14 further expanding at least one of said plain-text blocks and/or said first pseudo random

15 number into a set of pair-wise differentially-uniform pseudo random numbers;

16 combining said first pseudo random number, and/or said set of pair-wise

17 differentially-uniform pseudo random numbers, and/or said at least one plain-text block

18 to form at least two check sums and to re-form the said plain-text message; and

1   comparing said at least two check sums in declaring success of a message integrity check

2   in decryption of said cipher-text to reform said plain-text message.

3   33. An apparatus to encrypt a plain-text message, the apparatus comprising:

4   a Randomness Generator to generate a first random number;

5   a Randomness Transformer to transform said first random number into a first pseudo

6   random number;

7   a Pairwise Additively Uniform Sequence Generator to further expand a randomness of

8   said first random number and/or said first pseudo random number into a set of pair-wise

9   differentially-uniform pseudo random numbers;

10   an Encryptor to divide said plain-text message into a plurality of plain-text blocks, and to

11   encrypt said plain-text blocks to form a plurality of cipher-text blocks;

12   a Checksum Generator to combine said plurality of plain-text blocks into at least one

13   check sum; and

14   an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform

15   pseudo random numbers, together with said first random number and/or said first pseudo

16   random number, to embed a message integrity check in said cipher-text blocks.

17   34. An apparatus to decrypt a cipher-text message, the apparatus comprising:

18   a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks, and

19   to decrypt said cipher-text blocks in forming a plurality of plain-text blocks;

1   a Randomness Transformer to transform at least one of said plain-text blocks into a first

2   pseudo random number;

3   a Pairwise Additively Uniform Sequence Generator to further expand at least one of said

4   plain-text blocks and/or said first pseudo random number into a set of pair-wise

5   differentially-uniform pseudo random numbers;

6   a Checksum Generator to combine said first pseudo random number, and/or said set of

7   pair-wise differentially-uniform pseudo random numbers, and/or said at least one

8   plain-text block to form at least two check sums and to form a plurality of output blocks;

9   and

10   an Integrity Extractor and Checker to compare said at least two check sums in declaring

11   success of a message integrity check.

12   35. An article of manufacture comprising a computer usable medium having computer

13   readable program code means embodied therein for causing encryption of a plain-text

14   message, the computer readable program code means in said article of manufacture

15   comprising computer readable program code means for causing a computer to effect the

16   steps of claim 2 .

17   36. An article of manufacture comprising a computer usable medium having computer

18   readable program code means embodied therein for causing decryption of a cipher-text

19   message, the computer readable program code means in said article of manufacture

20   comprising computer readable program code means for causing a computer to effect the

21   steps of claim 14.

22   37. A computer program product comprising a computer usable medium having

23   computer readable program code means embodied therein for causing encryption of a

24   plain-text message, the computer readable program code means in said computer program

1   product comprising computer readable program code means for causing a computer to

2   effect the steps of claim 2.

3   38. A computer program product comprising a computer usable medium having

4   computer readable program code means embodied therein for causing decryption of a

5   plain-text message, the computer readable program code means in said computer program

6   product comprising computer readable program code means for causing a computer to

7   effect the steps of claim 14.

8   39. A program storage device readable by machine, tangibly embodying a program of

9   instructions executable by the machine to perform method steps for encrypting a

10   plain-text message, said method steps comprising the steps of claim 2.

11   40. A program storage device readable by machine, tangibly embodying a program of

12   instructions executable by the machine to perform method steps for decrypting a

13   cipher-text message, said method steps comprising the steps of claim 14.

14   41. A method as recited in claim 3, wherein the step of combining each pair includes

15   performing an addition in a group upon components of said each pair.

16   42. A method as recited in claim 11, wherein the step of combining each pair includes

17   performing an addition in a group upon components of said each pair

18   43. A method as recited in claim 15, wherein the step of using each pair includes

19   performing an addition in a group upon components of said each pair.

20   44. A method as recited in claim 21, wherein the step of combining each pair includes

21   performing an exclusive-or operation upon components of said each pair.

1   45. A method as recited in claim 21, wherein the step of combining each pair includes

2   performing an addition in a group upon components of said each pair.